ABSTRACT

An integrated circuit comprising a processor and memory storing: secret information accessible via a first address, the secret information comprising a string of bit values; an inverse-string accessible via a second address, the inverse-string comprising a string of bit values, wherein each of the bit values in the inverse-string is the logical inverse of a bit value at a corresponding bit position in the secret information, the integrated circuit being programmed with code configured to: (i) receive a request for the secret information; and (ii) test whether the bit-values of the inverse string are the inverse of the bit-values at respective corresponding bit positions of the secret information.